



FortiOS - Release Notes

VERSION 5.2.10

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



April 10, 2017

FortiOS 5.2.10 Release Notes

01-5210-396687-20170410

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
Last Release of Software	7
Special Notices	8
Local report customization removed	8
Compatibility with FortiOS versions	8
Removed WANOPT, NETSCAN, FEXP features from USB-A	8
Router Prefix Sanity Check	9
WAN Optimization in FortiOS 5.2.4	9
Built-In Certificate	9
FortiGate-92D High Availability in Interface Mode	9
Default log setting change	9
FG-5001D operating in FortiController or Dual FortiController mode	9
FortiGate units running 5.2.10	10
Firewall services	10
FortiPresence	10
SSL VPN setting page	10
Use of dedicated management interfaces (mgmt1 and mgmt2)	10
Upgrade Information	11
Upgrading from FortiOS 5.2.8 or later	11
Upgrading from FortiOS 5.0.13 or later	11
Web filter log options change from disabled to enabled after upgrade	11
Downgrading to previous firmware versions	11
FortiGate VM firmware	12
Firmware image checksums	12
Product Integration and Support	13
FortiOS 5.2.10 support	13
Language support	15
SSL VPN support	16
SSL VPN standalone client	16
SSL VPN web mode	16
SSL VPN host compatibility list	17

Resolved Issues 19

Known Issues 25

Limitations 28

 Citrix XenServer limitations 28

 Open Source XenServer limitations 28

Change Log

Date	Change Description
2016-11-29	Initial release.
2016-12-02	Updated <i>Supported Models</i> section.
2017-02-08	Added <i>Product Integration & Support > FSSO > 5.0 Build 0254 > Windows Server 2016 Standard</i> .
2017-03-01	Added 389206 to <i>Resolved Issues</i> .
2017-03-22	Removed 273910 from <i>Known Issues</i> .
2017-03-30	Added 356181 to <i>Resolved Issues</i> .
2017-04-10	Added <i>Special Notices > Use of dedicated management interfaces (mgmt1 and mgmt2)</i> .

Introduction

This document provides the following information for FortiOS 5.2.10 build 0742:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

See the [Fortinet Document Library](#) for FortiOS documentation.

Supported models

FortiOS 5.2.10 supports the following models.

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG-621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3950B and FCR-5001B FortiOS Carrier 5.2.10 images are delivered upon request and are not available on the customer support firmware download page. FortiOS Carrier firmware image file names begin with <i>FK</i> .

The following models are released on a special branch based off of FortiOS 5.2.10. As such, the *System > Dashboard > Status* page and the output from the `get system status` CLI command displays the build number.



FGT-VM64-AWS/AWSONDEMAND

Released on build 9428.

FGT-VM64-AZURE

Released on build 5817.

FG-5001B

Released on build 5819.

FG-5001C

Released on build 5819.

FG-5001D

Released on build 5819.

FG-5101C

Released on build 5819.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0742.



The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0742-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0742-FORTINET.out image.

Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the [Fortinet Customer Support portal](#):

Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

Special Notices

Local report customization removed

Local report customization has been removed from FortiOS 5.2. You can still record and view local reports, but you can no longer customize their appearance. For more control over customizing local reports, you can use FortiAnalyzer or FortiCloud.

Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

Removed WANOPT, NETSCAN, FEXP features from USB-A

The following features have been removed from the FortiGate and FortiWiFi 80C, 80CM, and 81CM:

- WAN Optimization
- Vulnerability scanning
- Using FortiExplorer on a smartphone to manage the device by connecting to the USB-A port

Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the [FortiOS 5.2.4 Feature Platform Matrix](#) to check the availability for your FortiGate model.

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used as the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to

the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

FortiGate units running 5.2.10

FortiGate units running 5.2.10 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

For the latest information, see the [FortiManager and FortiOS Compatibility](#).

Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
    set admin-https-ssl-versions tls1-0 tls1-1 tls1-2
end
```

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the [How to purchase and import a signed SSL certificate](#) document.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Upgrade Information

Upgrading from FortiOS 5.2.8 or later

FortiOS version 5.2.10 officially supports upgrade from version 5.2.8 or later.

Upgrading from FortiOS 5.0.13 or later

FortiOS version 5.2.10 officially supports upgrade from version 5.0.13 or later.



When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to [FortiOS 5.2 Supported Upgrade Paths](#)

Web filter log options change from disabled to enabled after upgrade

After upgrading from FortiOS 5.0.12 or 5.0.14 to FortiOS 5.2.10, all log options for web filter change from disabled to enabled, except the `log-all-url` option.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.2.10 support

The following table lists 5.2.10 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 42• Google Chrome version 46• Apple Safari version 7.0 (For Mac OS X) <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
Explicit Web Proxy Browser	<ul style="list-style-type: none">• Microsoft Internet Explorer versions 8, 9, 10, and 11• Mozilla Firefox version 27• Apple Safari version 6.0 (For Mac OS X)• Google Chrome version 34 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiManager	<p>For the latest information, see the FortiManager and FortiOS Compatibility.</p> <p>You should upgrade your FortiManager prior to upgrading the FortiGate.</p>
FortiAnalyzer	<p>For the latest information, see the FortiAnalyzer and FortiOS Compatibility.</p> <p>You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.</p>
FortiClient Microsoft Windows and FortiClient Mac OS X	<ul style="list-style-type: none">• 5.4.0 and later• 5.2.5 and later
FortiClient iOS	<ul style="list-style-type: none">• 5.4.1• 5.2.2 and later
FortiClient Android and FortiClient VPN Android	<ul style="list-style-type: none">• 5.2.8• 5.2.7

FortiAP

- 5.2.5 and later
- 5.0.10

You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller > Managed Access Points > Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.

FortiSwitch OS (FortiLink support)

- 3.4.2 build 0192
- Supported models: all FortiSwitch D models.

FortiSwitch-ATCA

- 5.0.3 and later
- Supported models: FS-5003A, FS-5003B

FortiController

- 5.2.0 and later
- Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
- 5.0.3 and later
- Supported model: FCTL-5103B

FortiSandbox

- 2.2.1
- 2.1.0

Fortinet Single Sign-On (FSSO)

- 5.0 build 0254 (needed for FSSO agent support OU in group filters)
 - Windows Server 2008 (64-bit)
 - Windows Server 2008 R2 64-bit
 - Windows Server 2012 Standard
 - Windows Server 2012 R2 Standard
 - Windows Server 2016 Standard
 - Novell eDirectory 8.8
- 4.3 build 0164 (contact [Support](#) for download)
 - Windows Server 2003 R2 (32-bit and 64-bit)
 - Windows Server 2008 (32-bit and 64-bit)
 - Windows Server 2008 R2 64-bit
 - Windows Server 2012 Standard Edition
 - Windows Server 2012 R2
 - Novell eDirectory 8.8

FSSO does not currently support IPv6.

FortiExplorer

- 2.6 build 1083 and later.

Some FortiGate models may be supported on specific FortiExplorer versions.

FortiExplorer iOS	<ul style="list-style-type: none"> 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	<ul style="list-style-type: none"> 3.0.0 build 0069 2.0.0 build 0003 and later
AV Engine	<ul style="list-style-type: none"> 5.177
IPS Engine	<ul style="list-style-type: none"> 3.174
Virtualization Environments	
Citrix	<ul style="list-style-type: none"> XenServer version 5.6 Service Pack 2 XenServer version 6.0 and later
Linux KVM	<ul style="list-style-type: none"> RHEL 7.1/Ubuntu 12.04 and later CentOS 6.4 (qemu 0.12.1) and later
Microsoft	<ul style="list-style-type: none"> Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	<ul style="list-style-type: none"> XenServer version 3.4.3 XenServer version 4.1 and later
VMware	<ul style="list-style-type: none"> ESX versions 4.0 and 4.1 ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓

Language	GUI
Korean	✓
Portuguese (Brazil)	✓
Spanish (Spain)	✓

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2328
Microsoft Windows 10 (32 bit & 64 bit)	2329
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2328
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2328

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit)	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33

Operating System	Web Browser
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/62bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox 42
Mac OS 10.9	Safari 7
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center 8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011		
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓

Product	Antivirus	Firewall
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

Resolved Issues

The following issues have been fixed in version 5.2.10. For inquiries about a particular bug, please contact [Customer Service & Support](#).

FortiAP

Bug ID	Description
381602	AUSTRALIA should use region code <i>N</i>

FortiGate 1500D

Bug ID	Description
386683	FG-1500D kernel panics after roughly 24 hours of uptime

FortiSwitch

Bug ID	Description
376375	FortiSwitch with B0181 (v3.4.1) can be discovered, but may be unable to obtain the IP address and be successfully authorized

AV

Bug ID	Description
389464	Flow-AV failed to detect <i>eicar</i> file if <code>ssl-exempt</code> entries exceed 140
384520	Chunk decoding causes segmentation fault because of incorrect pointer calculation

FOC

Bug ID	Description
382343	GTPv2 <code>Create-Session-Response</code> message with non-accepted <code>Cause</code> value should be allowed, even if the mandatory IE <code>Bearer-Context</code> is missing

FSSO

Bug ID	Description
386021	FSSO local poller fails on some X86 32 platform

GUI

Bug ID	Description
388759	Can't view interface list via VDOM
290997	Missing <i>Enable IPsec Interface Mode</i> from GUI for <code>pof_admin</code> when VDOM enabled
389417	Cannot display firewall policies from GUI in VDOM root
370360	VDOM read-only admin can view super admin and other higher privilege admin's password hash via REST API and direct URL
292210	Error 174 when changing administrator's profile
363546	Error 500 when saving urfilter list with 4900 entries
385482	GUI is loading indefinitely when accessing a "none" access web page from custom admin profile

HA

Bug ID	Description
385999	Log backup of <code>execute backup disk xxx</code> feature does not work fine on HA master unit
387212	HA gets out of sync frequently and hasync becomes zombie
389861	SNMP query for <code>fgHaStatsSyncStatus</code> on slave unit reports master as unsynchronized-"0"
275426	Re-sync can't be triggered when rebooting master and making some configuration changes on slave
367158	FortiGate HA configuration failed to sync issue with fsso-polling

IPS

Bug ID	Description
392045	Update the default built-in IPS engine in FOS 5.2

IPsec VPN

Bug ID	Description
391038	Memory leak discovered with valgrind in IKEv2

Bug ID	Description
380629	fnbamd matches wrong peer corresponding to a phase1 associated to a different IPSEC local-gw
376135	DHCP process is crashing when more than 1500+ users connect via dial up IPsec VPN with DHCP over IPsec feature enabled.
387677	NP2 not offloading IPsec VPN traffic

Kernel

Bug ID	Description
395515	ICMP unreachable message processing causes high CPU usage in kernel and DHCP daemon

Log/Report

Bug ID	Description
385659	Make value of <code>local-in-deny</code> setting keep consistent with the value from previous build after upgrade
280894	Remove GUI support for report customization and add feature store option for local reporting
380611 385115	Miglogd constantly crashing after upgrade to 5.2.8
373221	Can't clear log disk

Router

Bug ID	Description
391240	BGP UPDATES without NEXT_HOP

SLBC

Bug ID	Description
356181	The <code>confsyncd</code> uses 99% CPU when connection error is happening

SSL VPN

Bug ID	Description
385274 388657	Upgrade OpenSSL to 1.0.2j
371933	Unable to connect to SMB server that supports only NTLMv2

System

Bug ID	Description
287871	Administrative HTTPS and SSLVPN access using second WAN interface does not work after upgrade to 5.2.9
388032	Corrupted packets may cause malfunction of NP6, which causes NP ports to be unable to accept and forward traffic. Affected models: All NP6 platforms.
386876	Update geoip database to version 1.055(20161004)
276843	XG2 aggregate get very poor performance after enable <code>npu-cascade-cluster</code>
385897	The time, date and time are displayed differently in log
387675	ARP-Reply packets drops in NP6
389194	End of Daylight Savings (DST) timezone Turkey/Istanbul GMT +3
390088	Contract registration should accept characters
370151	CPU doesn't remove dirty flag when returns session back to NP6
378207	authd process running high CPU when only RSSO logging is configured
369372	With low latency mode on NP6 unit enabled, only first 2 packets are correctly processed by FortiGate
389398	<code>Can't find xitem. Drop the response</code> in dhcp relay debug
382996	Redundant type of interfaces are changing to aggregate after VDOM configuration restored
388603	After reassembling fragmented UDP packet, the s/d port become 0
376144	FortiManager failed to change FortiGate HA slave to master
283952	VLAN interface Rx bytes statistics higher than underlying aggregate interface
294198	Console prints out <code>NP6: No lacp_trunk interface</code>

Tablesize

Bug ID	Description
390053	Increase <code>firewall.schedule</code> limits on higher end

User

Bug ID	Description
373031	Unable to view FortiToken CD (FTK211) on FortiGate WebUI
294983	Radius Accounting do not follow <code>use-management-vdom enable</code> setting in Radius
374494	Tacacs+ <i>Test</i> button does not use set source-ip x.x.x.x

VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message

VoIP

Bug ID	Description
382315	SIP re-invites causing excessive memory consumption in imd

WebProxy

Bug ID	Description
371991	<code>YouTube_Video.Play</code> is not recognized with HTTPS in Application control Override
384581	Explicit Proxy Signing Certificate for replacement pages resets to default
387083	Constant Proxyworker crash with signal 8
304561	Proxyworker crashes on SMTP spamfilter
278318	only the first interface can work on web-proxy policy

Common Vulnerabilities and Exposures

Bug ID	Description
389206	<p>FortiOS 5.2.10 is no longer vulnerable to the following CVE References:</p> <ul style="list-style-type: none">• 2016-2177• 2016-2177• 2016-2178• 2016-2179• 2016-2180• 2016-2181• 2016-2182• 2016-2183• 2016-6302• 2016-6303• 2016-6304• 2016-6306 <p>Visit https://fortiguard.com/psirt for more information.</p>

Known Issues

The following issues have been identified in version 5.2.10. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Anti-spam

Bug ID	Description
374283	Spamfilter does not leave Anti-Spam log for the exempted traffic by bwl matching.

FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic sharper enabled on FortiGate-3810D TP mode.

FortiGate 3815D

Bug ID	Description
385860	FGT-3815D does not support 1GE SFP transceivers.

FortiSandbox

Bug ID	Description
273244	On the FortiGate device in <i>FortiView</i> > <i>FortiSandbox</i> , the analysis result may show a pending status and the FortiCloud side may show an unknown status.
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. <i>FortiView</i> > <i>FortiSandbox</i> may still show files are submitted even after the daily upload quota has been reached.

GUI

Bug ID	Description
310930	LDAP browser in <code>LDAP-group-GUI</code> may not respect group filter from LDAP server.
286226	Users may not be able to create new address objects from the Firewall Policy.

Bug ID	Description
285813	When navigating <code>FortiView > Application</code> some security action filters may not work.
278638	Explicit policy may be automatically reset to log security events.
271113	When creating an <code>id_based</code> policy with SSL enabled, and the <code>set gui-multipleutm disable</code> is applied, an <i>Entry not found</i> error message may appear.
268346	<i>All sessions: filter application, threat, and threat type</i> , may not work as expected
246546	Adding an override application signature may cause all category settings to be lost.
215890	Local-category status display may not change after running <code>unset category-over-ride</code> in the CLI.

System

Bug ID	Description
302272	Medium type may be shown incorrectly on shared ports.
285981	Adding more than eight members to <code>LACP get np6_lacp_add_slave</code> may result in an error.
285520	On NP4 platforms, TCP traffic may not be able to be offloaded in the decryption direction.
263864	When the interface is configured with <i>Auto-Speed</i> , FG-3240C NP4 Port 1G may stay down after reboot. Workaround: Set the interface speed to <i>1000/Full</i> .

VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl.

Webfilter

Bug ID	Description
380119	Webfilter static URL filter blocks additional domains with similar names.
378277	YouTube header injection (replacement for YouTube for Schools) was deleted.
284661	If the requested URL has port number, the URL filter may not block properly.

WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy.
355335	SSID may stop broadcasting.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
 - XVA (recommended)
 - VHD
 - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



FORTINET®

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.